Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Original) A biometric sensing system comprising:

an image capture device configured to capture images of an applied finger over a predetermined period of time and create a plurality of electrical representations of the applied finger;

a spoof detection module configured to analyse the plurality of electrical representations for relative temporal anomalies of intensity, or relative temporal anomalies of density, as measured between the plurality of electrical representations, indicative of a living applied finger; and

a minutia matching module for finding matches between the electrical representation of the applied finger.

2. (Original) The biometric sensing system of claim 1, wherein the spoof detection module is configured to employ an average intensity technique to detect and classify the anomalies, the average intensity technique configured to cause the system to calculate an average intensity for each of the plurality of electrical representations.

3. (Original) The biometric sensing system of claim 2, wherein the average intensity technique is further configured to cause the system to accept the applied finger as a living finger when the average intensity increases monotonically over the plurality of electrical representations.

4. (Original) The biometric sensing system of claim 1, wherein the spoof detection module is configured to employ a pixel density technique to detect and classify the anomalies, the pixel density technique causing the system to determine an ON-pixel value based upon a first electrical representation, determine pixel count for each electrical representation in the

plurality of electrical representations, wherein the counted pixels exceed the ON-pixel value, and calculate a delta pixel count of the plurality of electrical representations.

5. (Original) The biometric sensing system of claim 4, wherein the pixel density technique is further configured to cause the system to accept the applied finger as a living finger when the delta pixel count increases monotonically over the plurality of electrical representations.

6. (Currently Amended) The biometric sensing system of claim 1, wherein the spoof detection module is configured to employ a ridge uniformity technique to detect and classify the anomalies, the ridge uniformity technique configured to cause the system to measure pixel intensity along ridges in each of the plurality of electrical representations, determine whether the pixel intensity increases in a spatially non-uniform manner, and accept the applied finger as a living finger when the pixel intensity does ~~not~~ increase in the spatially ~~specially~~ non-uniform manner.

7. (Currently Amended) ~~The biometric sensing system of claim 1,~~ A biometric sensing system comprising:

an image capture device configured to capture images of an applied finger over a predetermined period of time and create a plurality of electrical representations of the applied finger;

a spoof detection module configured to analyse the plurality of electrical representations for relative temporal anomalies of intensity, or relative temporal anomalies of density, as measured between the plurality of electrical representations, indicative of a living applied finger; and

a minutia matching module for finding matches between the electrical representation of the applied finger;

wherein the spoof detection module is configured to employ a ridge uniformity technique to detect and classify the anomalies, the ridge uniformity technique configured to cause the system to measure pixel intensity values along contours of ridges in each of the plurality of electrical representations, binarize the pixel intensity values, measure the pixel intensity variations ~~various~~

along the ridges, and accept the applied finger as a living finger when the measured pixel intensity variations are roughly sinusoidal.

8. (Currently Amended) ~~The biometric sensing system of claim 1,~~ A biometric sensing system comprising:

an image capture device configured to capture images of an applied finger over a predetermined period of time and create a plurality of electrical representations of the applied finger;

a spoof detection module configured to analyse the plurality of electrical representations for relative temporal anomalies of intensity, or relative temporal anomalies of density, as measured between the plurality of electrical representations, indicative of a living applied finger; and

a minutia matching module for finding matches between the electrical representation of the applied finger;

wherein the spoof detection module is configured to employ a water droplet differential technique to detect and classify the anomalies, the water droplet differential technique configured to cause the system to locate a first water droplet positioned within an electrical representation in the plurality of electrical representations, locate a like-positioned water droplet within a subsequent electrical representation of the plurality of electrical representations, compare a size of the first water droplet with a size of the like-positioned water droplet, and accept the applied finger as a living finger when the size of the like-positioned water droplet is larger than the size of the first water droplet.

9. (Currently Amended) ~~The biometric sensing system of claim 1,~~ A biometric sensing system comprising:

an image capture device configured to capture images of an applied finger over a predetermined period of time and create a plurality of electrical representations of the applied finger;

a spoof detection module configured to analyse the plurality of electrical representations for relative temporal anomalies of intensity, or relative temporal anomalies of density, as measured between the plurality of electrical representations, indicative of a living applied finger; and

a minutia matching module for finding matches between the electrical representation of the applied finger;

wherein the spoof detection module is configured to employ a fingerprint vitality technique to detect and classify the anomalies, the fingerprint vitality technique configured to cause the system to compare a total swing ratio between the plurality of electrical representations.

10. (Original) The biometric sensing system of claim 9, wherein the fingerprint vitality technique is further configured to cause the system to compare a minimum or a maximum growth ratio between the plurality of electrical representations.

11. (Original) The biometric sensing system of claim 9, wherein the fingerprint vitality technique is further configured to cause the system to compare last to first fingerprint signal difference mean between the plurality of electrical representations.

12. (Original) The biometric sensing system of claim 9, wherein the fingerprint vitality technique is further configured to cause the system to compare a percentage change of standard deviation between the plurality of electrical representations.

13. (Original) The biometric sensing system of claim 9, further comprising a neural network, wherein the neural network is configured to perform the step of comparing.

14. (Original) A computer implemented method for detecting a spoof of a living finger, comprising:

capturing images of an applied finger over a predetermined period of time;

creating a plurality of electrical representations of the applied finger using the captured images;

analysing relative temporal anomalies of intensity or relative temporal anomalies of density for each of the plurality of electrical representations; and

matching minutia of the electrical representation of the applied finger, when the step of analyzing indicates that the applied finger is a living finger.

15. (Original) The method of claim 14, wherein the step of analyzing comprises:

calculating an average intensity for each of the plurality of electrical representations accepting the applied finger as a living finger when the average intensity, as sequentially measured over the plurality of electrical representations increases monotonically.

16. (Currently Amended) The method of claim 15, further comprising:

calculating an average change in the average intensity of the plurality of electrical representations; and

accepting the applied finger as a living finger when the average change in the average intensity is greater than a threshold average change in the average intensity value.

17. (Currently Amended) The method of claim 14, wherein the step of analyzing comprises:

selecting a portion of a first image in the plurality of electrical representations;

determining an ON-pixel value based upon intensity values in the portion of the first image;

counting a number of pixels exceeding the ON-pixel value in the portion of the first image;

repeating the above steps of selecting, determining, and counting for a next image in the plurality of electrical representations;

calculating an average density value between the first image and the next image; and

accepting the applied finger as a living finger when the average density value increases monotonically.

18. (Original) The method of claim 17, further comprising:

calculating an average change in average density between the plurality of electrical representations; and accepting the applied finger a living finger when

the average change in average density is less than a threshold average change in average density value.

19. (Original) The method of claim 14, wherein the step of analyzing comprises:

measuring intensity along ridges in each of the plurality of electrical representations;

comparing the intensity along the ridges from each electrical representation with the intensity along the ridges from a coterminously captured image;

determining whether the intensity along the ridges increases in a spatially non-uniform manner; and

accepting the applied finger as a living finger when the intensity along the ridges increases in a spatially non-uniform manner.

20. (Currently Amended) ~~The method of claim 14,~~ A computer implemented method for detecting a spoof of a living finger, comprising:

capturing images of an applied finger over a predetermined period of time;

creating a plurality of electrical representations of the applied finger using the captured images;

analysing relative temporal anomalies of intensity or relative temporal anomalies of density for each of the plurality of electrical representations; and

matching minutia of the electrical representation of the applied finger, when the step of analyzing indicates that the applied finger is a living finger;

wherein the step of analysing comprises:

locating water droplets in each of the plurality of electrical representations;

comparing a size of the water droplet in each of the plurality of electrical representations with a size of the water droplet in a subsequently captured image in the plurality of the electrical representations;

accepting the applied finger as a living finger when the water droplet size increases over time, as represented in the plurality of electrical representations.

21. (Currently Amended) ~~The method of claim 14,~~ A computer implemented method for detecting a spoof of a living finger, comprising:

capturing images of an applied finger over a predetermined period of time;

creating a plurality of electrical representations of the applied finger using the captured images;

analysing relative temporal anomalies of intensity or relative temporal anomalies of density for each of the plurality of electrical representations; and

matching minutia of the electrical representation of the applied finger, when the step of analyzing indicates that the applied finger is a living finger;

wherein the step of analysing comprises:

digitally processing a first electrical representation from the plurality of electrical representations;

saving the digitally processed electrical representation as a mask;

applying the mask over subsequent electrical representations;

converting the result of the mask of the subsequent electrical representatios into fingerprint strings;

connecting the fingerprint strings into a fingerprint signal for each image;

analysing the fingerprint signal for anomalies; and

accepting the fingerprint signal when the anomalies are indicative of a living finger.

22. (Original) The method of claim 21, wherein analysing the fingerprint signal for anomalies comprises calculating a total swing ration of a first fingerprint signal to a last fingerprint signal; and further comprising:

accepting the fingerprint signal when the total swing ratio is indicative of a living finger.

23. (Original) The method of claim 21, wherein analysing the fingerprint signal for anomalies comprises calculating a minimum or maximum growth ratio as measured between a first fingerprint signal and a last fingerprint signal; and further comprising:

accepting the fingerprint signal when the growth ratio is indicative of a living finger.

24. (Original) The method of claim 21, wherein analysing the fingerprint signal for anomalies comprises calculating a first fingerprint signal to a last fingerprint signal difference mean; and further comprising:

rejecting the fingerprint signal when the signal difference mean is indicative of a living finger.

25. (Original) The method of claim 21, wherein analysing the fingerprint signal for anomalies comprises calculating a percentage change of standard deviation between a first fingerprint signal and a last fingerprint signal; and further comprising:

accepting the fingerprint signal when the singal difference mean is indicative of a living finger.

26. (Original) The method of claims 21, further comprising:

calculating a spatial frequency of peaks in the fingerprint strings;

calculating a total energy for the fingerprint strings, based on the spatial frequency; and

accepting the fingerprint signal as a living finger when the average energy is above a threshold total energy.

27. (Original) The method of claim 21, further comprising, prior to accepting the fingerprint signal as a living finger, sending the anomalies to a neural network for classification.

28. (Currently Amended) A biometric sensing system comprising:

an image capture device configured to capture images of an applied object and create a plurality of electrical representations of the applied object;

a spoof detection module to extract minutia type information from ~~the~~ a first electrical representation, compare minutia type information with information corresponding to an enrolled object, calculate a ratio of mismatched minutia type information to matching minutia information, and reject the applied object as an inverted spoof when the ratio exceeds a threshold type mismatch ratio.

29. (Currently Amended) The biometric sensing system of claim 28, further comprising a minutia matching module configured to compare minutiae

extract from the first electrical representation of the applied object with minutiae of an enrolled object.

30. (Original) The biometric sensing system of claim 29, wherein the image capture device is a fingerprint sensor.

31. (Original) A computer implemented method for detecting a spoof of an applied object, comprising:

receiving one or more electrical representations representative of a plurality of images of the applied object;

extracting minutia type information from the one or more electrical representations;

determining whether the minutia type information matches a minutia type of a matching minutia from an enrolled object;

calculating a ratio of mismatched minutia types to matching minutia; and

rejecting the fingerprint signal as a spoof when the ratio of mismatched minutia types to matching minutia exceeds a threshold mismatch value.

32. (Original) The method of claim 31, further comprising:

capturing the plurality of images of the applied object with a fingerprint sensor; and

converting the plurality of images into the one or more electrical representations of the applied object.

33. (Original) The method of claim 32, further comprising matching minutiae extracted from at the one or more electrical representations with minutia from an enrolled object.

34. (Original) The method of claim 31, further comprising:

capturing the plurality of images of the applied object with a capacitive sensor; and

converting the plurality of images into the one or more electrical representations of the applied object.

35. (Original) The method of claim 34, further comprising matching minutiae extracted from at the one or more electrical representations with minutiae from an enrolled object.